REMARKS/ARGUMENTS

Favorable reconsideration of this application in light of the following discussion is respectfully requested.

Claims 1-12 are pending in the application. No claim amendments are presented, thus no new matter is added.

In the outstanding Official Action, Claims 1-6 and 9-10 were rejected under 35 U.S.C. § 103 as unpatentable over Levergood et al. (U.S. Patent No. 5,708,780, hereinafter "Levergood") in view of Ericsson, "Ericsson Helps Speed Up Mobile Browsing", InfoWorld article published May 31, 1999; and Claims 7, 8, 11 and 12 were rejected under 35 U.S.C. § 103 as unpatentable over Levergood and Ericsson and in further view of Wan (U.S. Patent No. 6,044,069, hereinafter "Wan").

The Official Action rejected Claims 1-6 and 9-10 under 35 U.S.C. § 103 as unpatentable over Levergood in view of Ericsson. The Official Action cites Levergood as disclosing the Applicant's claimed features with the exception of a client being in the form of a mobile information terminal. The Official Action cites Ericsson as enabling users of mobile telephones to connect to the internet and states that it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings of the cited references to arrive at Applicant's claims. Applicant respectfully traverses the rejection and asserts that Levergood fails to teach or suggest the claimed features for which it is asserted as a primary reference under 35 U.S.C. § 103.

Claim 1 relates to an authentication server which executes user authentication between a mobile information terminal and a content providing server connected by a data network. In advance of authentication, unique identification information stored in the mobile information terminal is registered with a customer database of an authentication server. Then, the unique identification information is encrypted by a predetermined encryption

algorithm and supplied from the mobile information terminal, via the network, and decoded by the authentication server. The server then determines whether the unique identification information decoded in the decoding step is registered with the customer database. After this determination is made, a notification is then sent to the content providing server to facilitate the start of services for the mobile information terminal.

Specifically, Claim 1 recites, *inter alia*, user authentication method, comprising:

> "... registering unique identification information stored in said mobile information terminal with a customer database of said authentication server in advance;
> decoding the unique identification information encrypted by a predetermined encryption algorithm and supplied from said mobile information terminal via said open network;
> determining whether the unique identification information decoded in the decoding step is registered with said customer database..."

This method allows a user of a mobile information terminal, or mobile phone, to provide user authentication without the need to input additional information, for example a password and user name to be authenticated at a server.

The requirements for a *prima facie* case of obviousness are (1) there must be some suggestion or motivation in the references themselves or in the knowledge generally available to one of ordinary skill in the art to modify the reference or to combine the reference teachings, (2) there must be a reasonable expectation of success, and (3) the prior art reference must teach or suggest all the claim limitations. It is respectfully submitted that the outstanding Official Action fails to make a *prima facie* case of obviousness, because neither Levergood nor Ericsson, alone or in combination, teach or suggest the claimed registering step, decoding step or determining step.

Levergood describes an internet server access control and monitoring system. Specifically, when a user of a client device selects a link directed to an access control file, the server subjects the request to a secondary server which determines whether the client has

authorization or a valid account to access this link.[1] Upon verification, the user is provided with a session identification (SID) which allows the user to access the requested file as well as another files within a present protection domain.

Specifically, Levergood describes that a SID is required in order to gain access to a specified link, the SID includes, among other things, a digital signature which is a cryptographic hash of the items in the SID and an authorized IP address which are both encrypted with a secret key and shared by the authentication and content servers.[2] In order to obtain a valid SID, the user must first be authenticated by an account database (216) using various non-encrypted parameters. If the user is authorized, a SID is generated allowing the user to gain access to the content.[3] However, Levergood describes that the SID is only generated upon the authentication of a user by the account database (216), and that no SID information is registered in the authentication server and stored in the client device in advance.

Claim 1 recites the step of registering unique identification information stored in a mobile information terminal with a customer database of an authentication server in advance. Levergood describes that information such as client IP address and password, as well as user demographic information, such as user age, home address, hobby or occupation may be stored in the content server.[4] Such information may be considered unique identification information. However, it should further be noted that no additional information, which may be considered unique identification information, is stored in the client device and the customer database of the authentication server in Levergood in advance of authenication.

Claim 1 further recites a step of decoding the unique identification information encrypted by a predetermined encryption algorithm and supplied from the mobile information

[1] Levergood at Abstract.
[2] Levergood at col. 5, lines 54-65.
[3] Levergood at col. 6, line 58 – col. 9, line 6.
[4] Levergood at col. 6, lines 60-65.

terminal over a network. Levergood fails to teach or suggest this claimed feature. In contrast, the only information in Levergood described as being encrypted and decoded is the SID, which is not stored in the mobile information terminal and the authentication server in advance.

In contrast, the SID in Levergood is generated after the client device is authenticated (using the user-parameters stored in the customer database 216) so that the user may obtain a SID to access specific information during a specified session. Thus, the SID is not stored in the client device and customer database in advance. Only the data used for authentication is stored in advance, and none of the authentication information (such as user demographic information, usernames and password) is/are encrypted and supplied from the client device to be decoded by the authentication server, as recited in Claim 1.

Further, as Ericsson is relied upon only to describe the ability of a mobile phone to connect over the internet to a server device, Applicant respectfully submits that Ericsson fails to teach or suggest any of the above-noted features recited in Claim 1.

Accordingly, Applicant respectfully requests the rejection of Claim 1 under 35 U.S.C. § 103 be withdrawn. For substantially the same reasons as given with respect to Claim 1, it is also submitted that Claim 9 patentably defines over Levergood and/or Ericsson.

Claims 7, 8, 11 and 12 were rejected under 35 U.S.C. § 103 as unpatentable over Levergood, Ericsson and in further view of Wan. Applicant respectfully traverses this rejection.

As discussed above, Levergood, neither alone nor in combination with Ericsson, teach or suggest an authentication server which registers unique identification information stored in a mobile information terminal with a customer database of the authentication server in advance and decodes the unique identification information encrypted by a predetermined encryption algorithm and supplied from the mobile information terminal. Likewise, Wan

fails to remedy this deficiency, and therefore, none of the cited references either alone or in combination, teach or suggest Applicant's Claims 7, 8, 11 and 12 which include the above distinguished limitation by virtue of independent recitation or dependency. Therefore, the Official Action fails to provide a *prima facie* case of obviousness with regard to any of these claims.

Accordingly, Applicant respectfully requests the rejection of Claims 7, 8, 11 and 12 under 35 U.S.C. § 103 be withdrawn.

Consequently, in light of the foregoing comments, it is respectfully submitted that the invention defined by Claims 1-12 is patentably distinguishing over the applied references. The present application is therefore believed to be in condition for formal allowance and an early and favorable reconsideration of the application is therefore requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Bradley D. Lytle
Attorney of Record
Registration No. 40,073

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 06/04)
ATH:smi
I:\ATTY\ATH\PROSECUTION\21'S\212668-US\212668US-AM.DOC